BUREAU OF CONSUMER PROTECTION Consumer Facts

Protecting Wisconsin Consumers for 75 Years

Imposter Scams

Beware! Imposters are everywhere! When the phone rings do you know who is calling before you answer or who sent the mail you just opened? When at your computer or on your smart phone do you know who sent the email in your inbox? Do you know who created that pop up message on your screen? All of these methods and many more are being used by scammers who are not what they may seem to be.

Signs of an Imposter Scam

Here are some common indicators that you are dealing with an imposter:

- **Requests for personal information.** Examples include: date of birth, social security number, Medicare ID number, credit card numbers, or bank account numbers.

- **Requests for payment of any kind**. No contest, prize or grant recipients have to make payment to receive their winnings or award.

- **Requests for payment by wiring money or pre-paid debit cards.** Providing money through either of these is the same as giving someone cash and it is not likely that it can be traced or retrieved once given.

- **Threats and urgency.** The more threatening the call – you'll be arrested, have to go to court, have your credit ruined the more likely it is from an imposter. Calls requiring urgent action from someone you do not know are likely made by imposters.

- **Requests for secrecy.** This is especially true for appeals for financial assistance from relatives who say "Don't tell my mom and dad." Or for calls about winning a prize where you are told by the caller you can't tell anyone else about it until you have received your winnings.

Imposter Phone Scams

- **IRS or Department of Treasury.** Threatening calls that you must pay now for tax violations. **The IRS will not contact you by phone. They would contact you by mail. They will not make threats.**

- **Federal Grant Award.** Do not be fooled by the 202 area code look like the call is coming from Washington, D.C. These unsolicited grants are not awarded. In the rare case where someone receives a grant they did not apply for**, no payment is required to receive the grant.**

- **Medicare or Affordable Health Care Act.** The caller claims to be a government representative insisting that you provide personal identification information and/or pay a fee or face loss of benefits. **Government agencies will contact you by mail, not by phone. They will not make threats on the phone.**

- **Other Law Enforcement or Government Agency.** The caller may threaten deportation but for a fee will assist you to get your certification. They hope you will be scared enough to part with money and/or personal identification information. Or a caller may claim that a foreign dignitary who needs your help with a money transfer is "legitimate". **No law enforcement or government agency makes these kinds of calls.**

- **Lottery or Prize Winner.** Often these calls come from an 876 area code, which is Jamaica. The caller says you have won but an administrative

fee, shipping, or taxes need to be paid. **You never have to pay for a prize or winnings.**

- **Family Assistance.** Also known as the "Grandparents Scam". These callers prey on the goodwill and desire to help family. The caller will say they are a family member, usually a younger one, in some kind of trouble needing immediate financial assistance. These scammers will feed off of information you inadvertently give them. **The caller will ask you not to call someone who could verify the legitimacy of the call** ("Don't call mom or dad") and to send money in an untraceable manner.

- **Computer Problems.** The caller claims to be from "Microsoft" or "Google" or another known company and states they have detected a problem with your computer. The caller may tell you to look in a particular place in your computer where you will see many error messages. The caller will tell you this is because of a virus or other problem with your computer. **The error messages you are seeing are completely normal on any properly functioning computer.** These callers will attempt to get you to pay for services, likely via credit card and to give access to your computer so they can steal personal information and download damaging software known as "malware" that will continue to allow access and even control of your computer**.** None of these companies make these kinds of calls. **Never give a caller access to your computer unless you are sure you know who is on the other side of the phone.**

- **Utility shut off.** The caller states you haven't paid your utility bill and someone is on the way over to disconnect your service unless you make an immediate payment to the caller. These calls target small businesses but some consumers report receiving these calls at home. To check if what the caller says is true, **call the number on your billing statement, not the number the caller gives you.**

- **"Spoofed" Numbers.** Technology exists that allows a caller to control what shows up on Caller ID. This is called **"spoofing"**. Calls may appear to come from a governmental agency, company or even a neighbor when actually the calls are coming from outside the country**. If you do not recognize the number on the Caller ID, let the call go to your answering machine or voicemail.** If it is important or a personal call, the caller will leave a message. If you have a question about the message left, call the Consumer Protection Hotline at 1-800-422-7128.

Imposter Mail Scams

Mail scams require a response once you've received the mail. The most common imposter scams are prize scams where you are instructed to call and told that you need to make a payment of some sort to receive you winnings. Versions of the phone imposter scams may also come in the mail or through email.

Imposter Computer Scams

- **Email scams.** Email imposter scams may be versions of the imposter phone or mail scams. Often the objective may be to get you to click on a link that will ask you for personal information or to click on an attachment that will download a virus or other malware to your computer.

- **Screen Pop-Ups.** A message will pop up on your screen, usually claiming there is something wrong with your computer and telling you to click on the window for assistance. You will then be given information to contact someone to help you, possibly from a known company like "Microsoft" or "Google". This is a variation on the Computer Problem calls. Often the screen pop-up messages are the result of a virus that has been downloaded to your computer to get you to make contact with them rather than the calling you. Sometimes you may receive a call once this message appears or you click on the pop up window**. If an error message appears on your computer, contact someone you know and trust for help.** Do not click on pop-up windows reporting a problem with your computer.

- **Online search imposter scams.** When looking for assistance through an online search, be aware that some companies, including

scammers, have paid to have their links appear at the top of your search list. It is very easy to think you are talking to a representative of the actual company you want, or are on their website, only to find you are being asked to provide personal information, payment information and/or access to your computer. **Check the website address to make sure you are dealing with the real company.**

- **Online dating imposter scams.** Online dating makes it easier for a person to misrepresent them self. Fake or outdated photos may be used, personal histories enhanced or exaggerated, personal traits fabricated. With traditional dating it is possible to talk with friends, family members or acquaintances to check a person's reputation. Online dating does not usually make this possible. Once a scammer is confident they have your trust, they will start asking for money. They may tell you they need it to help get money the government owes them, cover the costs of a sudden illness, surgery, a robbery, accident, or job loss. It may be for them, or a daughter or son. They may ask for money to cover the cost of travel to finally meet face-to-face. You might get documents from an attorney as "proof" of their genuine intentions along with a promise to pay it back. **As real as the relationship seems, it is a scam and you lose the money sent.**

- **Social networking website imposter scams.** Treat links in messages on these sites as you would a link in an email message. If it looks suspicious, even if you know the source, it is best to delete it or mark it as junk. Hackers can break into accounts and send messages that look like they are from your friends, but are not. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. **Do not trust that a message is really from who it says it is from.**

Do Not Respond!

The best defense against all these imposter scam is to not respond.

- **Do not answer the call.** Use your Caller ID. If you do not recognize the number let it go to your answering machine or voicemail. If you do answer the call, hang up as soon as you realize this is not someone you want to talk with. Talking to these callers or calling them back will likely result in additional contacts from them and other scammers.

- **Delete email from unknown senders.** If you do not know who sent it, do not open it. Sometimes opening an email is enough to tell a scammer that this is a valid address and they will continue to send you email. **If you do not know who sent it, never click on a link or attachment in an email.**

- **Verify your search result.** Before acting on the result of an online search, check to make sure you are dealing with the company you want. **If you do make contact, watch for the signs of a scam.**

- **Do not call the verification number you are given.** Call the number on a billing statement, found in the phone book or reliable online directory. **Never check to see if something is legit using the number given to you on the call, mailer, email or message.**

Contact Us

For more information or to file a complaint, visit our website or contact the Bureau of Consumer Protection.

Bureau of Consumer Protection
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911

E-MAIL:
DATCPHotline@wi.gov

WEBSITE:
datcp.wi.gov

(800) 422-7128

FAX: (608) 224-4677

TTY: (608) 224-5058

I:\dtcp\common\Fact Sheets\ImposterScams214 05/16